Notice of Allowability	Application No.	Applicant(s)	
	09/892,240	QI ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *8/8/2006*.

2. ☒ The allowed claim(s) is/are *1,3,5,6,9-15,17,19,20,23-28 and 41-50*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date 8/2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Claims 1, 3, 5-6, 9-15, 17, 19-20, 23-28, and 41-50 are pending.

Information Disclosure Statement

Applicant's newly submitted IDS has been considered.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Lori Gordon on 8/17/2006. The amendments are to fix 112, second paragraph errors. As per MPEP 713.04 a separate interview summary form is not provided, as the substance of the interview has been included herein.

The application has been amended as follows:

AMEND THE FOLLOWING CLAIMS AS FOLLOW:

Claim 1 (currently amended):

A cryptography engine for performing cryptographic operations on an initial input data bit sequence, the initial input data bit sequence having a right portion and a left portion, the cryptographic engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

two-level multiplexer circuitry including

a first level having a first 2-1 multiplexer and a second 2-1 multiplexer, wherein the first 2-1 multiplexer receives the left portion of the initial input data bit sequence at a first input and a right portion of the input bit sequence for a previous cryptographic round at a second input and wherein the second 2-1 multiplexer receives the right portion of the initial input data bit sequence at a first input and the right portion of the input bit sequence for the previous cryptographic round at a second input, and

a second level having a third 2-1 multiplexer and a fourth 2-1 multiplexer, wherein the third 2-1 multiplexer receives the output of the first 2-1 multiplexer at a first input and a right portion of an output bit sequence for a previous cryptographic round at a second input and wherein the fourth 2-1 multiplexer receives the output of the second 2-1 multiplexer at a first input and a right portion of the input bit sequence for the previous cryptographic round at a second input;

a first and a second expansion logic, wherein the first expansion logic is configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to the right portion of the initial input data bit sequence;

permutation logic coupled to the second expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the right portion of the output bit sequence for the previous cryptographic round;

a substitution box (SBox) configured to transform a third bit sequence to a fourth bit sequence,

wherein the right portion of the output bit sequence for the current cryptographic round is the exclusive OR of the output of the third 2-1 multiplexer and the fourth bit sequence and the left portion of the output bit sequence for the current cryptographic round is the output of the fourth 2-1 multiplexer, and

wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the previous cryptographic round.

Claim 15 (currently amended):

An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on an initial input data bit sequence, the initial input data bit sequence having a right portion and a left portion, the cryptographic engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

two-level multiplexer circuitry including

a first level having a first 2-1 multiplexer and a second 2-1 multiplexer, wherein the first 2-1 multiplexer receives the left portion of the initial input data bit sequence at a first input and a right portion of the input bit sequence for a previous cryptographic round at a second input and wherein the second 2-1 multiplexer receives the right portion of the initial input data bit sequence at a first input and the right portion of the input bit sequence for the previous cryptographic round at a second input, and

a second level having a third 2-1 multiplexer and a fourth 2-1 multiplexer, wherein the third 2-1 multiplexer receives the output of the first 2-1 multiplexer at a first input and a right portion of an output bit sequence for a previous cryptographic round at

a second input and wherein the fourth 2-1 multiplexer receives the output of the second 2-1 multiplexer at a first input and a right portion of the input bit sequence for the previous cryptographic round at a second input;

a first and a second expansion logic, wherein the first expansion logic is configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to the right portion of the initial input data bit sequence;

permutation logic coupled to the second expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the right portion of the output bit sequence for the previous cryptographic round;

a substitution box (SBox) configured to transform a third bit sequence to a fourth bit sequence,

wherein the right portion of the output bit sequence for the current cryptographic round is the exclusive OR of the output of the third 2-1 multiplexer and the fourth bit sequence and the left portion of the output bit sequence for the current cryptographic round is the output of the fourth 2-1 multiplexer, and

wherein the two-level multiplexer is configured to swap the left portion of the output bit sequence of a previous cryptographic round with the right portion of the output bit sequence of the previous cryptographic round.

Claim 49 (currently amended):

The integrated circuit layout of claim 15, wherein the right portion of the initial input bit sequence is an inverse permutation of a first portion of an input data block and

the left portion of the initial input bit sequence is an inverse permutation of a second portion of the input data block.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100